(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００１－１３６１５９
（Ｐ２００１－１３６１５９Ａ）
(43)公開日　平成13年5月18日(2001.5.18)

(51)Int.Cl.⁷	識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｂ	7/24	Ｂ	5C064
Ｈ０４Ｂ　7/24		Ｈ０４Ｈ	1/00	Ｅ	5J104
Ｈ０４Ｈ　1/00				Ｈ	5K067
		Ｈ０４Ｎ	7/173　６２０	Ｚ	
Ｈ０４Ｎ　7/173　６２０		Ｈ０４Ｌ	9/00　６０１	Ｂ	

審査請求　未請求　請求項の数１１　ＯＬ　（全１１頁）

(21)出願番号　特願平11-311651

(22)出願日　平成11年11月1日(1999.11.1)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者　赤地　正光
東京都品川区北品川6丁目7番35号ソニー株式会社内

(74)代理人　100082740
弁理士　田辺　恵基

Ｆターム(参考)　5C064 BA01 BB05 BB07 BC10 BC17
BC22 BD08
5J104 AA01 AA16 BA03 EA01 EA04
JA03 NA02 PA04
5K067 AA30 BB00 CC12 CC13 DD17
EE07 HH36

(54)【発明の名称】情報伝送システム及び方法、送信装置及び受信装置

(57)【要約】
【課題】様々な受信制御を行い得る情報伝送システムを得る。
【解決手段】受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにした。

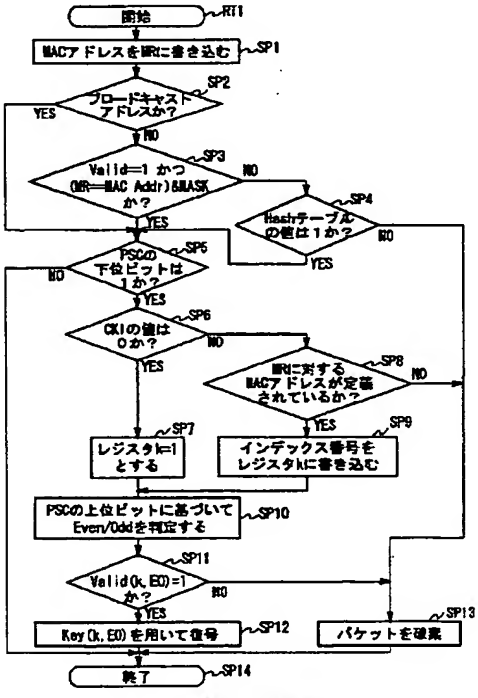

図６　復号処理

【特許請求の範囲】

【請求項１】送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送システムにおいて、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する上記送信装置と、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する上記受信装置とを具えることを特徴とする情報伝送システム。

【請求項２】上記送信装置は、上記複数の上記受信装置全てにデータを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信し、

上記受信装置は、受信した上記データに上記同報アドレスが付せられているとき、当該データを復号することを特徴とする請求項１に記載の情報伝送システム。

【請求項３】上記受信装置は、上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行うことを特徴とする請求項１に記載の情報伝送システム。

【請求項４】上記送信装置は、上記受信装置に対して個別にデータを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化し、

上記受信装置は、当該受信装置に対して個別に送信されたデータを、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて復号するとともに、任意のグループの上記受信装置間に対して送信されたデータを、上記共通鍵を用いて復号することを特徴とする請求項１に記載の情報伝送システム。

【請求項５】送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する送信ステップと、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する受信ステップとを具えることを特徴とする情報伝送方法。

【請求項６】それぞれ固有のアドレスを有する複数の受信装置にデータを送信する送信装置において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信することを特徴とする送信装置。

【請求項７】上記複数の上記受信装置全てに上記データを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信することを特徴とする請求項６に記載の送信装置。

【請求項８】上記受信装置に対して個別に上記データを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化することを特徴とする請求項６に記載の送信装置。

【請求項９】所定の送信装置から送信されたデータを受信して復号する受信装置において、

受信した上記データに付せられたアドレスと、当該受信装置固有のアドレスとが一致したとき、又は、受信した上記データに付せられた、複数の上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と当該アドレスの共通部分の範囲を指定するアドレス範囲情報とに基づいて、固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号することを特徴とする受信装置。

【請求項１０】受信した上記データに所定の同報アドレスが付せられているとき、当該データを復号することを特徴とする請求項９に記載の受信装置。

【請求項１１】上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行うことを特徴とする請求項９に記載の受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報伝送システム及び方法、送信装置及び受信装置に関し、例えば衛星を介して情報を伝送する情報伝送システムに適用して好適なものである。

【０００２】

【従来の技術】従来ディジタル衛星放送システムにおいては、受信契約を行った正当な受信者のみが放送を受信し得る限定受信機構（ＣＡ：Conditional Access）が用いられている。

【０００３】かかる限定受信機構においては、受信契約を行った受信者に対して予め所定の秘密鍵を渡しておく。送信側はこの秘密鍵を用いて放送データを暗号化し、放送衛星を介して送信する。そして受信者は秘密鍵を用いて受信波の暗号化を解除することにより、受信契約を行った受信者のみが放送を視聴し得るようになされている。

【０００４】

【発明が解決しようとする課題】ここで近年、ディジタル衛星放送システムを用いてデータ伝送を行う、衛星データ伝送システムが考えられている。衛星回線は電話回線やＩＳＤＮ回線等に比べてその通信速度が速いため、大容量データを短時間で伝送することができという利点がある。

【０００５】この衛星データ伝送システムにおいて、各受信者に対して個別のデータを伝送する個別通信（以下、これをユニキャストと呼ぶ）ことに加えて、全ての受信者に対して同一のデータを伝送する同報通信（以下、これをブロードキャストと呼ぶ）や、任意の受信者グループに対して同一のデータを伝送するグループ通信（以下、これをマルチキャストと呼ぶ）等の様々な受信制御を行うことができれば、衛星データ伝送システムの使い勝手がより一層向上すると考えられる。

【０００６】ところがかかる限定受信機構においては、全受信者が常に同じ情報を受信して視聴することを前提として設計されているため、ユニキャストやマルチキャスト等の受信制御を行い得ないという問題があった。

【０００７】本発明は以上の点を考慮してなされたもので、様々な受信制御を行い得る情報伝送システム及び方法、送信装置及び受信装置を提案しようとするものである。

【０００８】

【課題を解決するための手段】かかる課題を解決するため本発明においては、送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにした。

【０００９】任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信し、受信装置では固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較し、比較結果が一致したとき当該データを復号するようにしたことにより、簡易な構成で様々な受信制御を行い得る。

【００１０】

【発明の実施の形態】以下図面について本発明の一実施の形態を詳述する。

【００１１】（１）衛星データ伝送システムの全体構成図１において、１は全体として本発明を適用した衛星データ伝送システムを示し、送信側システム２、衛星３、及び複数の同一構成でなる受信側システム４で構成される。送信側システム２と各受信側システム４とはそれぞれインターネット５を介して接続されている。また送信側システム２を管理するサービスプロバイダと各受信側システム４を所有する受信者との間では、予め当該衛星データ伝送システム１についての利用契約が結ばれている。

【００１２】送信側システム２においては、当該送信側システム２全体を制御する制御装置１０、回線接続装置１１、データサーバ１２及び送信処理装置１３がローカルネットワーク１４を介して接続されている。

【００１３】制御装置１０は、受信側装置４が有する情報処理装置２２から送信されたデータ読出要求を、回線接続装置１１を介して受信する。そして制御装置１０はデータ読出要求に応じて、データサーバ１２或いはインターネット５上のデータサーバ（図示せず）からデータを読み出し、送信処理装置１３に供給する。

【００１４】ここで送信処理装置１３は、受信側装置４の各情報処理装置２２に付せられた固有の識別番号であるＭＡＣ（Media Access Control：メディアアクセス制御）アドレスと、当該ＭＡＣアドレスに対応して設定された秘密鍵とを記述した暗号鍵対応表を有している。そして送信処理装置１３は秘密鍵対応表に基づいて、読み出されたデータをデータ送信先の情報処理装置２２のＭＡＣアドレスに対応した秘密鍵を用いてデータを暗号化する。また送信処理装置１３は、ブロードキャストとして全ての情報処理装置２２に送信するデータについて、当該データのＣＫＩ（Common Key Indicator、後述）の

値を”０”とするとともに、所定の共通鍵を用いて暗号化する。そして送信処理装置１３は、暗号化したデータをＤＶＢ（Digital Video Broadcasting）データ放送仕様に定める形式でパケット化し、アップリンク波Ｓ２として送信１５を介して衛星３に送信する。

【００１５】衛星３はアップリンク波Ｓ２を受信して増幅し、ダウンリンク波Ｓ３として地上の受信側システム４に向けて再送信する。

【００１６】受信側システム４においては、受信装置２１、回線接続装置２３、及び、例えばパーソナルコンピュータ等でなる複数の情報処理装置２２が、ローカルネットワーク２４を介して相互に接続されている。

【００１７】受信装置２１は、受信アンテナ２０を介して受信したダウンリンク波Ｓ３に対して復調処理及び後述する復号処理を行うことにより、情報処理装置２２に向けに送信されたデータを復号し、ローカルネットワーク２４を介して、当該情報処理装置２２に供給する。

【００１８】また情報処理装置２２は、ユーザによってデータの読出要求操作が入力されると、これに応じてデータの読出要求を回線接続装置２３及びインターネット５を介して送信側システム２に送信する。

【００１９】（２）受信装置の構成

次に、受信側システム４の受信装置２１を図２を用いて説明する。

【００２０】受信装置２１においては、当該受信装置２１全体を制御するＣＰＵ（CentralProssecing Unit ）３０に、バス３９を介してフロントエンド部３１、分離部３２、受信フィルタ３３、復号部３４、チェッカ３５、バッファ３６、鍵テーブル３７及びインターフェース部３８が接続されている。

【００２１】フロントエンド部３１は、受信アンテナ３９を介して受信したダウンリンク波Ｓ３を復調し、データストリームＤ３１としてデマルチプレクサ３２に供給する。デマルチプレクサ３２は、ＰＩＤ（Packet ID ）に基づいて、データストリームＤ３１から必要なパケットのみを分離して受信フィルタ３３に供給する。受信フィルタ３３は、デマルチプレクサ３２から供給されたパケットのペイロード内容を調べ、データ復号処理に不要なパケットを破棄する。

【００２２】復号部３４は後述する復号処理に基づいて動作し、情報処理装置２２（図１）のＭＡＣアドレスを検索キーにして鍵テーブル２８に問い合わせを行い、当該鍵テーブル２８から復号鍵を取得する。そして復号部３４は、取得した復号鍵を用いてデータストリームＤ３１を復号し、復号データＤ３４としてチェッカ３５に供給する。

【００２３】チェッカ３５は、復号データＤ３４に対して復号処理が正常に行われたか否かの検査を行い、正常に復号されたパケットのみをバッファ３６に供給する。そしてバッファ３６はＣＰＵ３０の要求に応じて、復号データＤ３４をバス３９を介してインターフェイス部３８に読み出す。インターフェイス部３８は、復号データＤ３４をローカルネットワーク２４（図１）を介して情報処理装置２２に供給する。

【００２４】かくして受信装置２１はダウンリンク波Ｓ３を受信し、情報処理装置２２向けに供給されたデータのみを取り出して当該情報処理装置２２に供給する。

【００２５】（３）ディジタルストリームの復号処理

ディジタルストリームＤ３１は、図３に示すように、ペイロードの先頭にパケットヘッダ情報が付加されるとともに、ペイロードの末尾にスタッフィングバイト（無効バイト）及びＣＲＣ(Cyclic Redundancy Code ：巡回冗長符号）が付加され、ＤＶＢデータ放送仕様に定めるセッションとして処理可能な形態(Datagram-section)にカプセル化されて構成される。ここでＭＡＣアドレス＃６とは、ＭＡＣアドレスの最上位ビットをBit47 、最下位ビットをBit0としたときの、Bit7からBit0を含むバイト(8bit)を意味する。

【００２６】復号部３４においては、まず受信したデータストリームＤ３１の各パケットに記述されたＭＡＣアドレスと鍵テーブル３７とに基づいて、当該パケットを受信するべきか否かを弁別する。

【００２７】ここで本発明による受信装置２１は、かかるパケット弁別処理において、ＭＡＣアドレスにおける比較すべきビット位置を指定するマスクビット処理と、ＭＡＣアドレスをより少ないビット数の数値に変換し、これを用いてパケットの弁別を行うＭＡＣアドレス変換処理と、特定のＭＡＣアドレスを有するパケットを無条件で通過させるＭＡＣアドレス通過処理とを実行する。

【００２８】マスクビット処理は、セクションヘッダに記述されたＭＡＣアドレスと鍵テーブル３７のＭＡＣアドレスの比較演算による状態判定に、マスクビットと比較演算結果の論理積演算を付加するものであり、で、排他論理和を＾、論理積を＆で表し、セッションヘッダ記載のＭＡＣアドレスをＭＲ、鍵テーブルｋ番めのＭＡＣアドレスをＭＡＣ（ｋ）、ビットの重みを１と表すとすると、各ビット毎に

【００２９】

【数１】

$$(\sim(MR_i \hat{} MAC_i(k))) \& MASK_i(k) \quad \cdots\cdots (1)$$

【００３０】なる演算を０≦ｉ≦４７なる範囲で全てのビットに対して行い、この結果が全て”０”である場合にＭＡＣアドレスが合致したとするものである。

【００３１】これはすなわち、マスクが”１”であるビットにおいてのみＭＲとＭＡＣアドレスの比較を行うということである。このマスクビットとＭＲ及びＭＡＣアドレスの比較操作との関係を図４に示す。

【００３２】図４の場合、マスクビットはＤ０～Ｄ３ま

でが”０”であり、Ｄ４～Ｄ４７は”１”である。かかるマスクビットを用いてＭＡＣアドレスの照合を行う場合、マスクビットが”１”であるＤ４～Ｄ４７の区間において、ＭＡＣアドレスとＭＲが同一であることがＭＡＣアドレスの合致条件であり、マスクビットが”０”であるＤ０～Ｄ３の区間は、ＭＡＣアドレスとＭＲが同一でなくてもかまわない。このようにマスクビットを用いてＭＡＣアドレスの一部のみを照合することにより、それぞれ異なるＭＡＣアドレスを有する任意の情報処理装置２２に対して同一のパケットを配信するマルチキャスト（グループ通信）を行うことができる。またマスクビットを全て"1"、即ち"0xFFFFFFFFFFFF"とすることにより、ＭＡＣアドレス全てのビットに対して照合が行われ、ユニキャスト（個別通信）を行うことができる。

【００３３】ここで、マスクビットを用いてマルチキャストを行う場合、各情報処理装置２２のＭＡＣアドレスに共通部分が存在することが前提となるが、そのように情報処理装置２２を揃えることは難しく、またシステムを運用する際の柔軟さを欠くことにもなる。この場合、実際の情報処理装置２２のＭＡＣアドレスとパケットヘッダに記述されるＭＡＣアドレスとの対応表に基づいて、パケットヘッダを書き換えて疑似的にＭＡＣアドレスの共通部分を作り出すようにすればよい。

【００３４】ＭＡＣアドレス変換処理は、入力したＭＡＣアドレスに対してある種の計算式（ハッシュ関数）による演算を行い、４８ビット以下のビット数に縮小した数値を得、これをキーにして通過させるか否かを記述したテーブル（ハッシュテーブル）を検索するものである。このビット数の縮小は、ハッシュテーブルを小さくするためである。ハッシュ関数は入力されるＭＡＣアドレスをよく分散させるような関数であれば何でも良く、例えばＭＡＣアドレスのＣＲＣを求め、この上位６ビットをｐとし、Ｐａｓｓ（ｐ）が”１”であれば通過させ、例えば”０”であれば破棄する。ここでｐａｓｓは2^6＝６４ビットのテーブルである。このようにハッシュ関数を用いてＭＡＣアドレスのビット数を縮小することにより、復号部３４の回路規模を小さくすることができる。

【００３５】またＭＡＣアドレス通過処理は、パケットのヘッダに記述されたＭＡＣアドレスが所定の同報通信用のアドレスである場合、鍵テーブルの状態に関わらず通過させるというものであり、例えばパケットのヘッダ記載のＭＡＣアドレスが"0xFFFFFFFFFFFF"（このアドレスをブロードキャストアドレスと呼ぶ）であれば常に同報通信（ブロードキャスト）とみなしてこれを通過させる。本発明においては、かかるＭＡＣアドレス通過処理をマスクビット処理及びＭＡＣアドレス変換処理に先行して実行する。これによりパケットヘッダ記載のＭＡＣアドレスがブロードキャストアドレスである場合鍵テーブルの検索が不要になり、処理速度が向上するという効果がある。

【００３６】かくして復号部３４は、パケットのヘッダに記述されたＭＡＣアドレス、情報処理装置２１のＭＡＣアドレス、及びマスクビットに基づいてパケットの弁別を行う。

【００３７】続いて復号部３４は、弁別されたパケットが暗号化されているかを検出する。そしてパケットが暗号化されているときは、復号鍵を鍵テーブルより取り出して復号処理を行うが、同報通信においては複数のＭＡＣアドレスで共用する復号鍵である共通鍵を具備する必要がある。

【００３８】本発明による受信装置２１では、共通鍵を使用するか否かを、例えばセクション６バイト目の最上位ビット（図３の２行めの第２番目のバイトのＤ７）を用いて判断する。これを本発明ではＣＫＩ（Common Key Indicator）と呼ぶ。そしてＣＫＩが”１”であれば、ＭＲ、ＭＡＣアドレス及びマスクビットによって鍵テーブルから抽出される個別鍵を使用し、ＣＫＩが”０”であれば、鍵テーブルの設定にかかわらず共通鍵を使用すると定める。ここで、ＤＶＢデータ放送仕様においてはＣＫＩはｒｅｓｅｒｖｅｄとされており、値として”１”をとることになっている。共通鍵は個別鍵に比べてより特殊な処理方法であると考えられるので、ＣＫＩが”０”である場合に共通鍵を使用すると定めることで、ＤＶＢデータ放送仕様との仕様を一致することができる。

【００３９】共通鍵は特定の記憶領域を用意しても良いが、鍵テーブル中の特定の行のデータを兼用すれば処理が個別鍵と共通化でき、記憶領域も有効に利用できるのでより望ましい。この特定の行としてより好ましくは先頭の行、即ち第１行を指定する。鍵テーブルの行数ｎがいくつであれ必ず第１行めは存在するので、このようにすればｎの値が異なる受信装置であっても処理手順を変えることなく共通鍵の記憶又は取り出しを行うことができる。

【００４０】図５は鍵テーブルの構成を示し、ＭＡＣアドレス＃１は鍵テーブルの第１番行に記述されたＭＡＣアドレスを、マスク＃１はＭＡＣアドレス＃１に対応するマスクビットを、K_{1Even}、K_{1Odd}は各々ＭＡＣアドレス＃１に対応づけれたＥｖｅｎ／Ｏｄｄの鍵データを意味しており、使用する暗号形式に応じたビット幅ｍを持つ。鍵テーブルは上記と同様の構造を複数（ｎ個）持っている。この最大数は鍵テーブル２８が持ちうる回路規模から上限が決定される。

【００４１】ＭＡＣアドレスと鍵データはそれぞれ独立したＶａｌｉｄフラグを有しており、これにより個別に値が有効であるか無効であるかを管理することができるようになされており、当該Ｖａｌｉｄフラグを、ＭＡＣアドレス弁別に流用することも可能になる。また、鍵テーブルは各行毎に独立したＶａｌｉｄフラグを有してい

るため、当該鍵テーブルは空行（無効な行）を含んでいても良く、これにより一時的に特定の行の情報を無効にしたい場合、単にＭＡＣアドレスのＶａｌｉｄビットを”０”にするだけでよく、高速な処理のために好適である。

【００４２】復号部３４は、かくして得られた復号鍵を用いてパケットの復号を行う。

【００４３】（４）復号処理手順

次に、ディジタルストリームの復号処理手順を図６の流れ図に示しながら説明する。

【００４４】復号部３４はＲＴ１で処理を開始し、ステップＳＰ１において、パケットヘッダに記述されている４８ｂｉｔのＭＡＣアドレスをレジスタＭＲに読み込み、次のステップＳＰ２に進む。

【００４５】ステップＳＰ２において、復号部３４はレジスタＭＲの値がブロードキャストアドレス（0xFFFFFFFFFFFF）に等しいか否かを判断する。ステップＳＰ２において肯定結果が得られた場合、このことはレジスタＭＲの値がブロードキャストアドレスに等しいこと、すなわち当該パケットがブロードキャストパケットであることを表しており、復号部３４はステップＳＰ３及びＳＰ４をスキップし、ステップＳＰ５に進む。

【００４６】これに対してステップＳＰ２において否定結果が得られた場合、このことはレジスタＭＲの値がブロードキャストアドレスに等しくないこと、すなわち当該パケットがブロードキャストパケットではないことを表しており、復号部３４はステップＳＰ３に進む。

【００４７】ステップＳＰ３において、復号部３４は鍵テーブル３７内に、Ｖａｌｉｄビットが”１”（すなわち有効状態）であるとともに、マスクビットが”１”である区間の全ビットにおいてレジスタＭＲとＭＡＣアドレスとが等しい行が存在するか否かを、（１）式に基づいて鍵テーブルを＃１行から順に各行検索する。

【００４８】ステップＳＰ３において肯定結果が得られた場合、このことは有効状態かつマスクビットが”１”である区間の全ビットにおいてレジスタＭＲとＭＡＣアドレスとが等しい行が存在したことを表しており、復号部３４はステップＳＰ５に進む。

【００４９】これに対してステップＳＰ３において否定結果が得られた場合、このことは有効状態かつマスクビットが”１”である区間の全ビットにおいてレジスタＭＲとＭＡＣアドレスとが等しい行が存在しないことを表しており、復号部３４はステ４に進む。

【００５０】ステップＳＰ４において、復号部３４は、ハッシュ関数を用いてパケットヘッダに記載のＭＡＣアドレスからハッシュ値を生成し、当該ハッシュ値を用いて所定のハッシュテーブルを検索し、ハッシュ値に対応するビットが”１”であるか否かを判断する。

【００５１】ステップＳＰ４において否定結果が得られた場合、このことはハッシュテーブルのビットが”０”であり、当該パケットは受信装置２１が受信すべきパケットではないことを表しており、復号部３４はステップＳＰ１３に進み、当該パケットを破棄し、ステップＳＰ１４で処理を終了する。

【００５２】これに対してステップＳＰ４において肯定結果が得られた場合、このことはハッシュテーブルのビットが”１”であり、当該パケットは受信装置２１が受信すべきパケットであることを表しており、復号部３４はステップＳＰ５に進む。

【００５３】ステップＳＰ５において、復号部３４は、パケットヘッダにおけるＰＳＣ（Payload Scrambling Control）（図３）の下位ビットの値に基づいて、当該パケットが暗号化されているか否かを判断する。ステップＳＰ５において否定結果が得られた場合、このことは下位ビットが”０”であること、すなわち当該パケットが暗号化されていないことを表しており、復号部３４はステップＳＰ１４へ進み、暗号解除処理を行わずにパケットを後段のチェッカ３５に送出し処理を終了する。

【００５４】これに対してステップＳＰ５において肯定結果が得られた場合、このことは下位ビットが”１”であること、すなわち当該パケットが暗号化されていることを表しており、復号部３４はステップＳＰ６に進む。

【００５５】ステップＳＰ６において、復号部３４は、パケットヘッダにおけるＣＫＩ（図３）の値に基づいて、当該パケットが共通鍵を用いて暗号化されているか否かを判断する。ステップＳＰ６において肯定結果が得られた場合、このことはＣＫＩが”０”であること、すなわち当該パケットが共通鍵を用いて暗号化されていることを表しており、復号部３４はステップＳＰ７へ進み、鍵の索引番号を記憶するレジスタｋに共通鍵を示す”１”を代入し、ステップＳＰ１０に進む。

【００５６】これに対してステップＳＰ６において否定結果が得られた場合、このことはＣＫＩが”１”であること、すなわち当該パケットが個別鍵を用いて暗号化されていることを表しており、復号部３４はステップＳＰ８に進む。

【００５７】ステップＳＰ８において、復号部３４は鍵テーブルを（１）式に基づいて各行順次検索し、ＭＲに合致するＭＡＣアドレスが鍵テーブル上に存在するか否かを判断する。ここで、ステップＳＰ４におけるハッシュテーブルによる弁別では受信すべきではないパケットもたまたまハッシュ値が合致すれば通過させてしまうが、このようなパケットは当該ステップＳＰ８にて再度弁別されるため、誤って復号処理されることはない。ちなみに、暗号化されていないパケットはステップＳＰ８を通過しないので、これは後段回路あるいは情報処理装置２２にて破棄する。

【００５８】鍵テーブルの探索は、当該鍵テーブルの第１行から順に行われ、最初に合致するまで照合が繰り返される。ここで、有効なアドレスとは図５に示すＶａｌ

ｉｄビットが活性状態であるものである。例えばＶａｌｉｄビットが”１”の状態を活性状態とするならば、即ちＶａｌｉｄビットが”０”である行の情報は無効となる。例えばＭＡＣアドレス＃２のＶａｌｉｄビットが”０”であると、K_{2Even}、K_{2Odd}に何が設定されていてもこれらの値は参照されない。

【００５９】ステップＳＰ８において否定結果が得られた場合、このことはＭＲに合致するＭＡＣアドレスが鍵テーブル上に存在せず、当該パケットは受信装置２１が受信すべきパケットではないことを表しており、復号部３４はステップＳＰ１３に進み、当該パケットを破棄し、ステップＳＰ１４で処理を終了する。

【００６０】これに対してステップＳＰ８において肯定結果が得られた場合、このことはＭＲに合致するＭＡＣアドレスが鍵テーブル上に存在し、当該パケットは受信装置２１が受信すべきパケットであることを表しており、復号部３４はステップＳＰ９に進み、レジスタｋにＭＡＣアドレスが（１）式の条件下で合致した鍵の索引番号を代入し、ステップＳＰ１０へ進む。

【００６１】ステップＳＰ１０において、復号部３４はＰＳＣの上位ビットに基づいて、当該パケットがＥｖｅｎ期間の鍵で暗号化されているのかＯｄｄ期間の鍵で暗号化されていのかを判断する。例えばＰＳＣの上位ビットが”０”の場合にＥｖｅｎ期間、”１”の場合にＯｄｄ期間であると定める。

【００６２】そして復号部３４は、ＰＳＣの上位ビットが”０”であった場合は、合致したＭＡＣアドレス＃ｉに対応するＥｖｅｎ期間の鍵及びK_{iEven}のＶａｌｉｄビットの値を鍵テーブルから取り出し、ＰＳＣの上位ビットが”１”であった場合は、合致したＭＡＣアドレス＃ｉに対応するＯｄｄ期間の鍵及びK_{iOdd}のＶａｌｉｄビットの値を鍵テーブルから取り出し、次のステップＳＰ１１に進む。

【００６３】ステップＳＰ１１において、復号部３４は、取り出したＶａｌｉｄビットの値が、”１”であるか（すなわちＶａｌｉｄ（ｋ、ＥＯ）＝１）であるか否かを判断する。ステップＳＰ１１において否定結果が得られた場合、このことはＶａｌｉｄ（ｋ、ＥＯ）が”０”であること、すなわちパケットが暗号化されているにもかかわらず有効な復号鍵（個別鍵）が存在しないことを表しており、復号部３４はステップＳＰ１３に進んで当該パケットを破棄し、ステップＳＰ１４で処理を終了する。

【００６４】これに対してステップＳＰ１１において肯定結果が得られた場合、このことはＶａｌｉｄ（ｋ、ＥＯ）が”１”であること、すなわちパケットに対する有効な復号鍵（個別鍵）が存在することを表しており、復号部３４はステップＳＰ１２に進む。

【００６５】ステップＳＰ１２において復号部３４は、ＫＥＹ（ｋ、ＥＯ）すなわちｋ番めのＥＯに対応する復号鍵を鍵テーブル３７から取り出し、当該復号鍵を用いてパケットを復号して後段のチェッカ３５に出力し、ステップＳＰ１４で処理を終了する。

【００６６】かくして復号部３４は、鍵テーブル３７及びハッシュテーブルに基づいて、ユニキャスト、マルチキャスト及びブロードキャストの各配信形態に対応したパケット復号処理を行う。

【００６７】ここで、かかる復号処理における復号鍵の検索処理（ステップＳＰ５～ＳＰ１３）は、ＭＡＣアドレスの弁別処理（ステップＳＰ１～ＳＰ４）とは独立に処理されるため、ブロードキャストアドレスに対しても暗号化処理を行うことができる。この場合、共通鍵をブロードキャストアドレスに対する通信の復号鍵とする第１の方法と、ブロードキャストアドレスを個別鍵に対応するＭＡＣアドレスとして鍵テーブルへ登録する第２の方法の２つの共通鍵設定方法が考えられる。

【００６８】第１の方法では、鍵テーブル３７の記憶領域は消費しないが他の同報通信と鍵を共用しなければならない。第２の方法では鍵テーブルの記憶領域を消費するものの、ブロードキャスト専用の復号鍵を設定することができる。

【００６９】（５）実施の形態における動作及び効果
以上の構成において、復号部３４は、受信したデータストリームＤ３１の各パケットに記述されたＭＡＣアドレスに基づいて、ブロードキャストアドレス（”0xFFFFFFFFFFFF”）を有するパケットを弁別するとともに、マスクビットを用いたＭＡＣアドレスの照合を行い、マルチキャスト及びユニキャストのパケットを弁別する。このとき復号部３４はＭＡＣアドレスのハッシュ値を算出し、当該ハッシュ値に基づいてマルチキャスト及びユニキャストのパケット弁別を行う。

【００７０】そして復号部３４は、弁別されたパケットが暗号化されているかを検出し、当該パケットが暗号化されている場合、復号鍵を鍵テーブルより取り出して復号処理を行う。このとき復号部３４はパケットのＣＫＩに基づいて、当該パケットの暗号化が共通鍵によるものか個別鍵によるものかを判別し、これに応じて共通鍵又は個別鍵を用いてパケットを復号する。

【００７１】以上の構成によれば、特定のＭＡＣアドレスをブロードキャストアドレスとして用いるとともに、マスクビットを用いてＭＡＣアドレスの一部のビットのみを照合するようにしたことにより、ブロードキャスト、マルチキャスト及びユニキャストといった様々な受信制御を行うことができる。

【００７２】また、ハッシュ関数を用いてＭＡＣアドレスのビット数を縮小し、当該縮小したＭＡＣアドレスを用いてパケットの弁別を行うようにしたことにより、復号部３４の回路規模を縮小することができる。

【００７３】（６）他の実施の形態
なお上述の実施の形態においては、マスクビットが”

1”である位置のビットを、ＭＡＣアドレスの比較対象としたが、本発明はこれに限らず、逆にマスクビットが”０”である位置のビットをＭＡＣアドレスの比較対象とするようにしても良い。

【００７４】また上述の実施の形態においては、ハッシュテーブルを用いたパケットの弁別において、ハッシュテーブルの検索結果が”０”である場合にパケットを破棄するようにしたが、本発明はこれに限らず、逆にハッシュテーブルの検索結果が”１”である場合にパケットを破棄するようにハッシュテーブルを設定しても良い。

【００７５】さらに上述の実施の形態においては、ＭＡＣアドレス"0xFFFFFFFFFFFF"をブロードキャストアドレスとしたが、本発明はこれに限らず、これ以外のＭＡＣアドレス"0xFFFFFFFFFFFF"をブロードキャストアドレスとしても良い。

【００７６】さらに上述の実施の形態においては、復号処理においてブロードキャストアドレスの弁別（ステップＳＰ２）、鍵テーブルにおけるＭＡＣアドレスの照合（ステップＳＰ３）、ハッシュテーブルの検索（ステップＳＰ４）の順で処理を行うようにしたが、本発明はこれに限らず、これ以外の順序で復号処理を行うようにしても良い。

【００７７】さらに上述の実施の形態においては、衛星データ伝送システムに本発明を適用する場合について述べたが、本発明はこれに限らず、これ以外のデータ伝送システム、例えばケーブルインターネット等に適用しても良い。

【００７８】

【発明の効果】上述のように本発明によれば、受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにしたことにより、簡易な構成で様々な受信制御を行うことができる。

【図面の簡単な説明】

【図１】本発明による衛星データ伝送システムの全体構成を示すブロック図である。

【図２】受信装置の回路構成を示すブロック図である。

【図３】ヘッダフォーマットを示す略線図である。

【図４】マスクとＭＡＣアドレスの関係を示す略線図である。

【図５】鍵テーブルのデータ構成を示す略線図である。

【図６】復号処理を示すフローチャートである。

【符号の説明】

１……衛星データ伝送システム、２……送信側システム、３……衛星、４……受信側システム、５……インターネット、１０……制御装置、１１……回線接続装置、１２……データサーバ、１３……送信処理装置、１４……ローカルネットワーク、１５……送信アンテナ、２０……受信アンテナ、２１……受信装置、２２……情報処理装置、２３……回線接続装置、２４……ローカルネットワーク、３０……ＣＰＵ、３１……フロントエンド部、３２……デマルチプレクサ、３３……受信フィルタ、３４……復号部、３５……チェッカ、３６……バッファ、３７……鍵テーブル、３８……インターフェース部、３９……バス。

【図２】

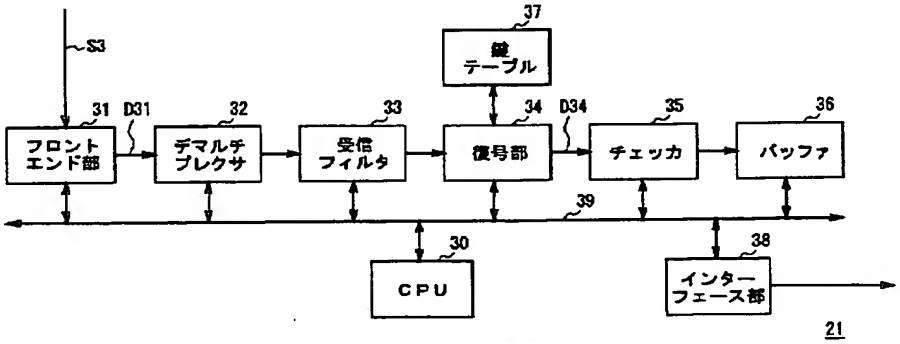

図２　受信装置

【図１】

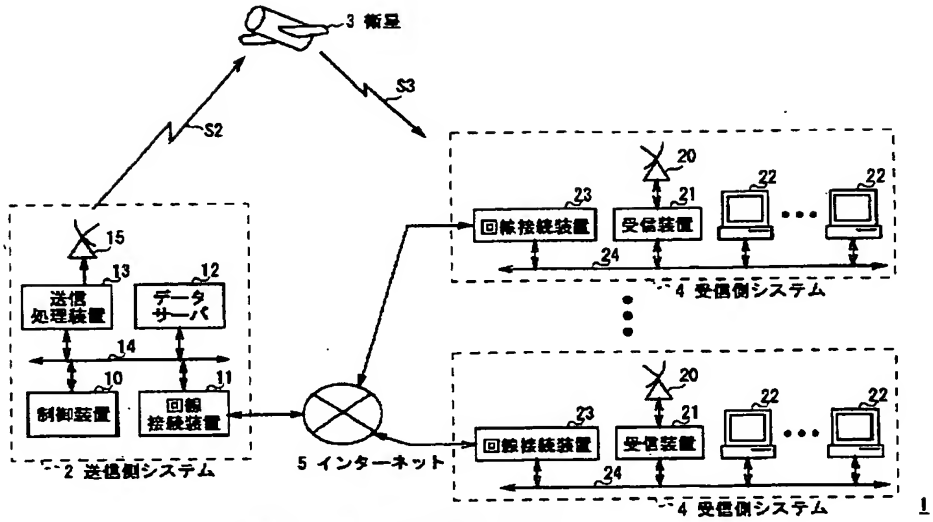

図１　衛星データ伝送システム

【図３】

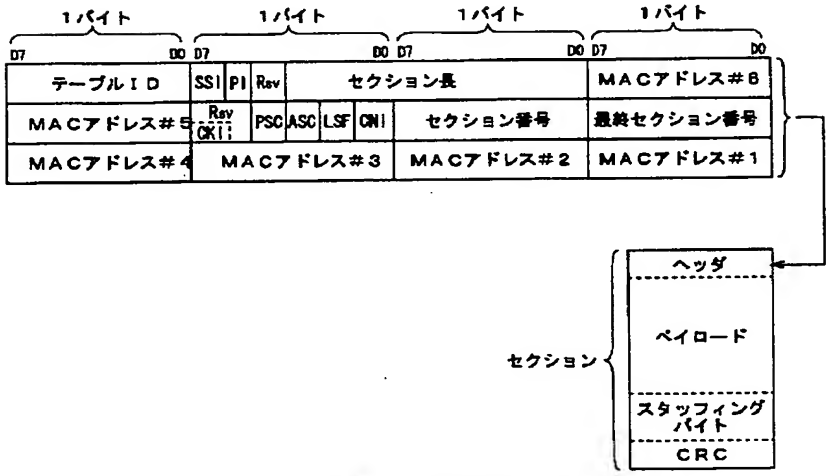

図３　ヘッダフォーマット

【図４】

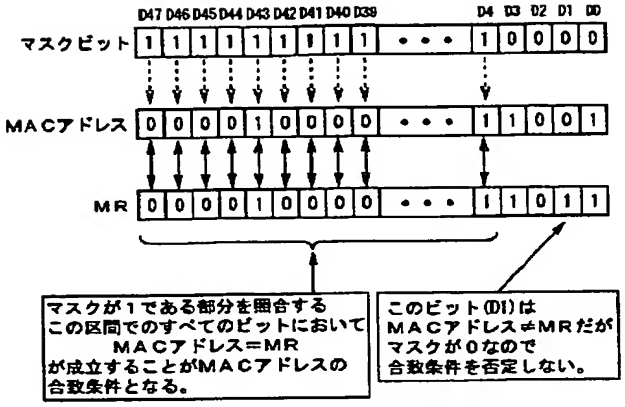

図４　マスクとＭＡＣアドレス

【図５】

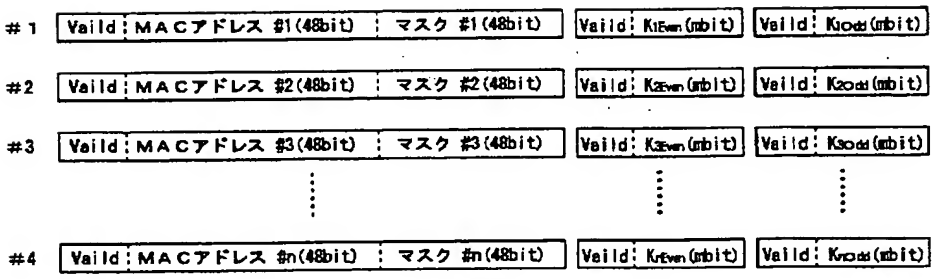

図５　鍵テーブル

【図６】

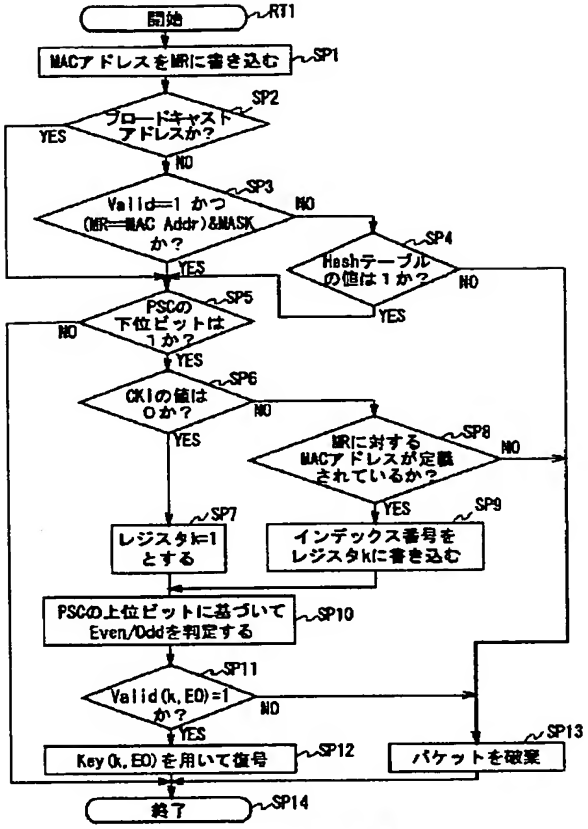
開始
RT1
MACアドレスをMRに書き込む
SP1
ブロードキャスト アドレスか?
SP2
YES
NO
Valid=1 かつ (MR=MAC Addr)&MASK か?
SP3
NO
YES
Hashテーブルの値は1か?
SP4
NO
YES
PSCの下位ビットは1か?
SP5
NO
YES
CKIの値は0か?
SP6
NO
YES
MRに対するMACアドレスが定義されているか?
SP8
NO
YES
レジスタk=1とする
SP7
インデックス番号をレジスタkに書き込む
SP9
PSCの上位ビットに基づいてEven/Oddを判定する
SP10
Valid(k,EO)=1か?
SP11
NO
YES
Key(k,EO)を用いて復号
SP12
パケットを破棄
SP13
終了
SP14

図６　復号処理